PGP® Support Package for BlackBerry®

Extending PGP® email security to enterprise handhelds

Part of the PGP® Encryption Platform

Extend, manage, and enforce PGP email security policies to BlackBerry device users

As the need for mobile data access increases, it is critical that mobile devices be protected within the enterprise security architecture. PGP Corporation and Research In Motion® (RIM®) have collaborated to develop PGP Support Package for BlackBerry, a comprehensive solution that extends PGP messaging security to BlackBerry devices.

Enable PGP-Secured Email on BlackBerry Devices

With PGP Support Package for BlackBerry, PGP-secured email messages are automatically encrypted, digitally signed, decrypted, and verified on BlackBerry devices:

- Combines PGP email security with the mobility and flexibility of BlackBerry devices.
- Provides sender-to-recipient PGP security capabilities for wireless mobile users.

Centrally Enforce Email Security

PGP Support Package for BlackBerry is fully interoperable with other PGP® Encryption Platform–enabled applications.

- Integrates into a comprehensive security solution for email, instant messaging (IM), and full disk and virtual volume encryption—all with a unified management console.
- Enables administrators to centrally define, manage, and enforce policy for PGP Encryption Platform–enabled applications.
- Consistently enforces messaging security policies, regardless of enterprise origination point (PC or BlackBerry) or message destination.

Enterprise Benefits

End-to-End PGP Security for Microsoft Exchange & Lotus Notes Users

Together with PGP Support Package for BlackBerry and a BlackBerry® Enterprise Server, PGP Universal™ Server enables BlackBerry users with Microsoft® Exchange or Lotus Notes® to employ end-to-end PGP messaging security.

Consistent Enforcement of Centralized Email Security Policies

Managed by PGP Universal Server policies, BlackBerry devices with PGP Support Package for BlackBerry automatically encrypt email based on existing email security policies. This approach enables the enterprise to enforce consistent security for both PC and device email clients.

Rapid, Simple Deployment

PGP Universal Server enables BlackBerry devices to automatically enroll in PGP Universal Server's Self-Managing Security Architecture. Over-the-air enrollment simplifies administrative requirements, reducing costs and deployment time.

Two-Way Policy Enforcement

Corporate email security policies can be extended to customers and business partners outside the corporate domain using PGP Universal Server's ad-hoc encryption capabilities.

Features

PGP Encryption on BlackBerry Devices

- PGP-secured email can be decrypted/verified and encrypted/digitally signed on BlackBerry devices for true sender-to-recipient secure messages.

- BlackBerry users no longer have to choose between using PGP security and using their BlackBerry devices because they can do both at the same time—transparently.

Auto-Fetching of PGP Keys

- PGP Support Package for BlackBerry automatically searches for recipient encryption keys during message composition, eliminating delays when sending PGP-secured messages.

Integration with BlackBerry Device Email Client

- PGP Support Package for BlackBerry is integrated with the BlackBerry device's native email client and leverages the BlackBerry device's existing security features. PGP Support is activated with a simple license update.

Managed Features

Assured Access

- PGP Universal Server management enables organizations to enforce the use of patented PGP Additional Decryption Key (ADK) technology for data access, according to policy.
- Ensures corporate access to encrypted data for regulatory or audit purposes.
- Decrypts messages encrypted by PGP keys within the organization.

Automatic & Transparent Operation

- PGP Universal Server encryption policies are automatically downloaded by the BlackBerry device.
- Message encryption and decryption are transparent to the user.

Key Management

- PGP Universal Server can generate, manage, and search for keys transparently, simplifying key management with virtually no end-user training requirements.

Automatic Key Lookup & Verification

- Automatic key lookup and verification removes the requirement for users to store message recipients' keys locally on the device before sending or verifying PGP-secured email.

S/MIME Integration

- PGP Universal Server security policies can be seamlessly applied to BlackBerry devices with S/MIME certificates.

Technical specifications

Device Specifications

- BlackBerry Handheld Software 4.1 or higher
- PGP® Desktop 8.x or greater (PGP Desktop 9.5 required for Lotus Notes environments)

Server Specifications

- MS Exchange environments: PGP Universal Server 2.02 or greater required for managed features
- BlackBerry Enterprise Server for Microsoft Exchange 4.0.2 or greater (4.1.2 required for PGP/MIME support)
- Lotus Notes environments: PGP Universal Server 2.5 or greater required for managed features
- BlackBerry Enterprise Server for Lotus Notes 4.1 or greater (4.1.2 required for PGP/MIME support)

(For current product specifications, see www.pgp.com/products/pgp_support_package_for_bb/tech_specs.html)

PGP and the PGP logo are registered trademarks of PGP Corporation. Product and brand names used in the document may be trademarks or registered trademarks of their respective owners. Any such trademarks or registered trademarks are the sole property of their respective owners.

PGP Corporation
www.pgp.com

PGP Corporate Headquarters
Tel: +1 650 319 9000

PGP (GB) Ltd.
Tel: +44(0) 208 622 3039

PGP Deutschland AG
Tel: +49 69 838310 0

PGP Japan K.K.
Tel: +81 03 4360 8308

© 2006 PGP Corporation
SP4BBDS060920